AF
ZZW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

First Named Inventor : Robert H. Thibadeau	Appeal No. ---
Appln. No. : 09/912,931	
Filed : July 25, 2001	Group Art Unit: 2136
For : METHODS AND SYSTEMS FOR PROMOTING SECURITY IN A COMPUTER SYSTEM EMPLOYING ATTACHED STORAGE DEVICES	Examiner: Primila Parthasarathy
Docket No.: S01.12-1058	

SUPPLEMENTAL BRIEF FOR APPELLANT

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I HEREBY CERTIFY THAT THIS PAPER IS BEING SENT BY U.S. MAIL, FIRST CLASS, TO THE COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450, THIS

12 DAY OF October, 2005

PATENT ATTORNEY

Sir:

This is an appeal from an Office Action dated February 17, 2005 in which claims 1 to 145 were finally rejected.

REAL PARTY IN INTEREST

Antique Books, Inc., a corporation organized under the laws of the state of Pennsylvania, and having offices at 2 Queens Court, Pittsburgh Pennsylvania 15228, has acquired the entire right, title and interest in and to the invention, the application, and any and all patents to be obtained therefor, as set forth in the Assignment filed with the patent application and recorded on Reel 013159, frame 0386.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

STATUS OF THE CLAIMS

I. Total number of claims in the application.

Claims in the application are: 1-145

II. Status of all the claims.

A.	Claims cancelled:	None
B.	Claims withdrawn but not cancelled:	None
C.	Claims pending:	1-145
D.	Claims allowed:	None
E.	Claims rejected:	1-145
F.	Claims Objected to:	None

III. Claims on appeal

The claims on appeal are: 1-145

STATUS OF AMENDMENTS

No amendment was filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

One embodiment of the present invention is directed to a method for promoting security in a computer system having an operating system. The computer system is connected with at least one storage device. An example of this aspect is shown in FIG. 1 of the present specification where computer 6 includes an operating system 10 and a storage device 12. As shown, for example, in FIG. 2, the storage device 12 includes a processor (indicated by CPU 18) and firmware 16 for processing data stored (in data storage 16) on the storage device 12. (*See* application at p. 9, lines 1-3). At least a portion of the storage device is partitioned to form a security partition having at least one authority record and at least one data set associated with said authority record. An example of this aspect is shown in FIG. 3 of the present specification where the security partition data 32 and authority records 34, 36, and 38 are "contained in a security partition of the storage device 30" (See application, p. 10, lines 3-9). Access to the security partition of the storage device by the operating system of the computer system is limited. An example of this aspect is discussed with respect to FIG. 3 in the present application at page 10, lines 14-21, as follows:

> Operations involving the authority records 34, 36, 38 are managed by the firmware of the storage device 30. In one embodiment, all authority records 34, 36, 38 can be governed by a single master authority record 40. As shown, an operating system ("OS") file system 42 is not permitted to access the security partition data 32 contained in the storage device 30. This independence of the security partition data 32 from the OS file system 42 provides an important benefit of the present security methods and systems: to create a location on a computer system where information such as a secret can be effectively concealed.

Another embodiment of the present invention is directed to a system for promoting security in a computer system having an operating system in operative connection with at least one storage device. An example of this aspect is shown in FIG. 1 where the computer system 6 has an operating system 10 in operative connection with storage device 12. The storage device includes a processor and firmware for processing data stored on the storage device. An example of this aspect is shown in FIG. 2, which illustrates the storage device 12 including a processor (indicated by CPU 18) and firmware 16 for processing data stored (in data storage 16) on the storage device 12. A security partition is formed in the storage device with at least one authority record and at least one data set associated with the authority record. An example of this aspect is shown in FIG. 3 of the present specification where the security partition data 32 and authority records 34, 36, and 38 are "contained in a security partition of the storage device 30" (See application, p. 10, lines 3-9). Access to the security partition of the storage device by the operating system of the computer system is limited. An example of this aspect is discussed with respect to FIG. 3 in the present application at page 10, lines 14-21 (reproduced above).

Another embodiment of the present invention is directed to a computer-readable medium containing instruction for promoting security in a computer system having an operating system in

operative connection with at least one storage device. An example of this aspect is illustrated in FIG. 1 where the computer system 6 has an operating system 10 in operative connection with storage device 12. The storage device includes a processor and firmware for processing data stored on the storage device. An example of this aspect is illustrated in FIG. 2, which illustrates the storage device 12 including a processor (indicated by CPU 18) and firmware 16 for processing data stored (in data storage 16) on the storage device 12. The storage medium includes instructions for partitioning at least a portion of the storage device to form a security partition having at least one authority record and at least one data set associated with said authority record. An example of this is illustrated in FIG. 3 of the present specification where the security partition data 32 and authority records 34, 36, and 38 are "contained in a security partition of the storage device 30" (See application, p. 10, lines 3-9). The storage medium includes instructions for limiting access to at least a portion of the storage device by the operating system of the computer system. An example of this aspect is illustrated in FIGS. 5-7, and is discussed in the specification at page 10, lines 16-18, and at page 13 line 5 through page 18, line 19.

Another embodiment of the present invention is directed to a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device. An example of this aspect is illustrated in FIGS. 1 and 2, where a computer system 6 has an operating system 10 coupled to a storage device 12, which includes a CPU 18, data storage 16 and firmware 14. The system includes a means for partitioning at least a portion of said storage device to form a security partition having at least one authority record and at least one

data set associated with said authority record. An example of this is shown in FIGS. 1 and 2 of the present invention as firmware 14, which manages operations involving the authority records 34, 36 and 38 within the security partition of the storage device 30. (*See* application p. 10, lines 14-15 and FIGS. 2 and 3). The system includes means for limiting access to the security partition of the storage device by the operating system of said computer system. An example of this aspect is illustrated as the firmware 14, which manages access to the security partition such that the operating system file system 42 "is not permitted to access the security partition data 32" contained in the security partition of the storage device 30. *See* FIGS. 2 and 3 and page 10, lines 14-21 (reproduced above).

Another embodiment of the present invention is directed to a storage device for promoting security in a computer system. The storage device includes a storage medium for storing data and firmware for reading data from and writing data to the storage medium. An example of this aspect is shown as firmware 14 and data storage 16 on storage device 12 in FIG. 1. The storage device includes a partition defined on the storage medium for dividing the storage medium into a data partition and a secure data partition, the secure data partition for storing secure data and one or more authority records. An example of this aspect is shown as security partition data 32 and authority records 34-38 as compared to operating system file system 42 in FIG. 3. (*See* application, p. 10, lines 3-13. Only the firmware of the storage device is permitted to access the secure data and the one or more authority records. An example of this feature is described at page 10, lines 14-21.

Another embodiment of the present invention is directed to a method for promoting security in a computer system having an operating system in operative connection with a storage device. The storage device includes a processor and firmware for

processing data stored on the storage device (*See* FIG. 2, CPU 18 and firmware 14 coupled to data storage 16 and page 9, lines 1-6). The method includes partitioning a storage medium of the storage device into a data partition and a secure data partition. An example of this aspect is shown in FIG. 3 as storage device 30, which is partitioned into a secure partition and a data partition. In this example, the secure partition contains security partition (SP) data 32, authority records 34, 36 and 38 and master authority record 40, and the data partition contains the OS file system 42. The data partition is accessible to a user and the secure data partition is invisible to the user. An example of this aspect is described at page 15, lines 14-18. The method also includes restricting access to the secure data partition such that only the firmware may access the secure data and the one or more authority records, which is described, for example, at page 10, lines 14-21.

Another embodiment of the present invention is directed to a storage device, including a storage medium having a security partition containing one or more authority records and at least one data set associated with each of the one or more authority records. An example of this aspect is illustrated in FIG. 3 as storage device 30 with a security partition containing authority records 34, 36 and 38 and security partition (SP) data 32. (*See also* application, page 10, lines 7-9). The storage device includes a mechanism within the storage device adapted to limit access to the security partition based on the one or more authority records. An example of this aspect is illustrated as firmware 14 in FIGS. 1 and 2, and is discussed at page 10, lines 14-21. For example, the firmware 14 manages operations involving the authority records, and the operating system file system 42 is not permitted to access the security partition data 32 (shown in FIG. 3) *See* p. 10, lines 14-21.

ISSUES

Whether claims 1-15, 20-24, 29, 32-42, 46-49, 53-70, 75-78, 82, 83, 86-103, 108-112, 116, 117, 120-128, and 130-145 (Appendix A) of the present application are novel over Diamant et al. (U.S. Patent No. 6,268,789) (hereinafter "the Diamant patent") (Appendix B).

Whether claims 16-19, 25-28, 30, 31, 43-45, 50-52, 71-74, 79-81, 84, 85, 104-107, 113-115, 118, 119, and 129 are non-obvious over the Diamant patent in view of Aucsmith et al. (U.S. Patent No. 5,940,513) (hereinafter "the Aucsmith patent") (Appendix C).

GROUPING OF THE CLAIMS

Appellant groups the claims on appeal as follows:

Group I = claims 141-145;

Group II = claims 132-136;

Group III = claims 123-131, 137; and

Group IV = claims 1-122, 138-140.

ARGUMENT

Group I.

Claims 141-145 were rejected under 35 U.S.C. 102(e) as being anticipated by the Diamant patent.

A. Group I Claims are Novel in View of the Diamant Patent.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). *See* MPEP 2131.

Independent claim 141 reads as follows:

A storage device comprising:
a storage medium having a security partition containing one or more authority records and at least one data set associated with each of the one or more authority records; and

> a mechanism within the storage device adapted to limit access to the security partition based on the one or more authority records.

(emphasis added). The Diamant patent does not teach or disclose a mechanism within the storage device adapted to limit access to the security partition. In particular, the Diamant patent teaches, for example, in FIGS. 1-4, 6, 7, 9-12 and 14, a controller that is external to the storage device for controlling access to the data stored on the storage device. This external controller (for example, controller 12 in FIG. 1, managing controller 98 in FIG. 2, and so on) is coupled to public network 6 and secured network 8, operates within server 4, and communicates with the storage device 14 via I/O interface 96. *See* the Diamant patent, Col. 7, line 60 through Col. 8, line 25). Moreover, the operating system of server 4 is common to the Internet. The Diamant patent reads as follows:

> The public network 6 is also connected to an external network which in the present example is the Internet 80.
>
> Server 4 includes a Central Processing Unit 10 (CPU), a storage unit 14 and a controller 12. The controller 12 is adapted to receive transmissions from networks 6 and 8 and write them in various locations in the storage unit 14.

See the Diamant patent, col. 5, lines 35-42. Thus, the Diamant patent teaches a mechanism that is external to the storage device. The Diamant patent does not teach or disclose a mechanism within the storage device that is adapted to limit access to the security partition.

The external controller of the Diamant patent represents a conventional system as described in the background of the present application as follows:

> Perhaps the greatest fundamental problem with conventional computer security systems is that their operation is common to the environment of the operating system environment. Furthermore, the operating system environment for many computer systems is also common to the Internet environment, for example, or another

> network communications medium. Because of this common environment, many means of attack on a computer system are available merely by moving computer code from the Internet to the computer operating system.
> ...
> Other conventional security systems may include a security device connected to an SCSI bus that protects storage devices on the bus. This type of security system recognizes that the storage device is more secure while not operating in an environment common to the operating system. However, the SCSI bus of this system exposes all devices on the bus, including the storage devices, to access and therefore requires intimate operating systems involvement.

See Application, p. 2, lines 1-20.

Further, the Diamant patent does not teach or disclose limiting "access to the security partition based on the one or more authority records", which are stored within the security partition. In fact, the Diamant patent teaches controlling access using an external controller based on the type of network from which the access request is received. For example, referring to node 30 in FIG. 1, the Diamant patent reads as follows:

> The communication controller 38 monitors all communication transmissions received from the public network so as to detect access attempts to the secured storage area 34. When such an attempt is detected, the communication controller denies access to the secured area 34 and executes an alert procedure to alert the user of the node 30.

See Col. 6, lines 8-14; *see also* Col. 5, lines 46-60. Thus, the external controller of the Diamant patent controls access to the secured area based on the type of network from which the access request is received, not "based on the one or more authority records" as recited in claim 141.

The Office Action states

> Diamant teaches and describes a storage device (Fig. 1-8, 11, 14 and Column 5 line 25-Column 15 line 22), comprising:
> a storage medium having a security partition containing one or more authority records and at least one data set

> associated with each of the one or more authority records (Fig. 2, 5, 8, 11, 14 and Column 5 line 25 - Column 6 line 60, Column 8 line 26-Column 9 line 31, Column 10 lines 18-53, Column 18 lines 5-12 and Column 21 lines 1-12), wherein the secured area contains data and confidential information...

(See Final Office Action, p. 7). However, the Diamant patent does not teach or disclose an authority record as described in the present application, nor does it teach or disclose a security partition containing the authority records.

In the present application, an embodiment of an authority record is shown, for example, in FIG. 4 and identified generally by reference numeral 52. The authority record 52 includes access rights 56, security partition name 58, passcode 60, public key out 62, public key in 64, symmetric key 66, write permission 68-72, read permissions 74-78, time field 80, encryption settings 82, start, size and number information 84, and secure data 54 associated with the authority record.

Appellant notes that the references cited by the Examiner do not teach or disclose and authority record within the security partition. The Diamant patent at Col. 5, line 25 through Col. 6, line 60 describes the operation of the external controllers. For example, the Diamant patent reads as follows:

> According to the invention, each of the communication controllers 12, 28, 38, 48 and 78 monitors all of the communication transmissions received from the public network 6 so as to detect access attempts to a respective secured storage area connected thereto. When such an attempt is detected, the respective communication controller denies access to the relevant secured area and executes an alert procedure to alert any user using a node or server.

See Col. 6, lines 46-54. The Diamant patent at Col. 8-Col. 9, Col. 10, and Col. 21 relate to the Diamant external controller. The Diamant patent at col. 8 line 26 through Col. 9 line 31 describes a controller adapted to deny access requests for access to secured data received from a public network (*See* Col. 9, lines 3-8 and lines 15-20). The Diamant patent at col. 10 lines 18-53 describes

an external device 300 that has a processor 302 for controlling switch 304 "so as to allow or deny access to the secured area 320". *See* Col. 10, lines 47-48. The Diamant patent at col. 18 line 5-12 describes a secured area 1130 containing "data and software which are confidential" and a separate password area 1133 containing "passwords which may be utilized during various procedures by the managing controller 1122, such as switching between modes and the like." The Diamant patent at col. 21, lines 1-12 describes how the "managing controller 1122 connects between the secured area 1130 and the computer 1102, thus enabling the computer to load an operating system from the secured area 1130." The cited portion at Col. 18 lines 5-12 relate to passcodes, which are stored in a passcode area 1133 area of the storage device 1124 in FIG. 14. The passcode information is stored separately from the secured area 1130 and apparently without association to the secured area 1130. The Diamant patent does not teach or disclose storage of passcodes or of authority records within the secure data area as recited in independent claim 141.

Therefore, the Diamant patent does not teach or disclose all the elements of independent claim 141. Claim 141 is novel in view of the cited art. Claims 142-145 depend from allowable independent claim 141. The Diamant patent does not teach or disclose all the elements of claims 142-145, which are therefore allowable over the cited art.

Group II.

Claims 132-136 were rejected under 35 U.S.C. 102(e) as being unpatentable over the Diamant patent.

A. Group II Claims are Novel in View of the Diamant Patent.

Independent claim 132 reads as follows:

> A method for promoting security in a computer system having an operating system in operative connection with a storage device, wherein said storage device includes a processor and firmware for processing data stored on the

> storage device, the method comprising:
>
> partitioning a storage medium of the storage device into a data partition and a secure data partition, the data partition being accessible to a user and the secure data partition being invisible to the user, the secure data partition for storing secure data and one or more authority records; and
>
> restricting access to the secure data partition such that only the firmware may access the secure data and the one or more authority records.

(emphasis added). As previously discussed, the Diamant patent does not teach or disclose "a secure data partition for storing … one or more authority records" as recited in claim 132.

Additionally, the Diamant patent does not teach or disclose a storage device including a processor and firmware and "restricting access to the secure data partition such that only the firmware may access the secure data and the one or more authority records" as recited in claim 132. Specifically, the Diamant patent teaches an external controller that controls access to the secured area. The Diamant patent does not teach or disclose restricting access "such that only the firmware may access the secure data" as recited in claim 132.

Further, the Diamant patent does not teach or disclose hiding or making the secure data partition "invisible to the user" as recited in the claims. An example of this aspect is discussed in the application at page 15, lines 14-18. Though the external controller of the Diamant patent prevents non-secured nodes from accessing secured data (*See* the Diamant patent, col. 6, lines 32-35), there is no indication in the Diamant patent that such data is invisible. At Col. 18, lines 53-64, the Diamant patent mentions that addresses beginning 0,0,#, except 0,0,1 are not used by programs designed for IBM-PC architecture. There is no indication that such addresses are invisible to a user. Therefore, the Diamant patent does not teach or disclose

all the elements of independent claim 132. Independent claim 132 is novel in view of the cited art.

Claims 133-136 depend from allowable independent claim 132. The Diamant patent does not teach or disclose all the elements of claims 132; and therefore, all the elements of claims 133-136 are not taught or disclosed by the Diamant patent. Therefore, claims 133-136 are allowable over the cited art.

Group III.

Claims 123-128, 130, 131 and 137 were rejected under 35 U.S.C. 102(e) as being anticipated by the Diamant patent. Claim 129 was rejected under 35 U.S.C. 103(a) as being unpatentable over the Diamant patent in view of the Aucsmith patent.

A. Claims 123-128, 130-131 AND 137 Are Novel in View of the Diamant patent.

Independent claim 123 reads as follows:

> 123. (Previously Added) A storage device for promoting security in a computer system, the storage device comprising:
>
> a storage medium for storing data;
>
> firmware for reading data from and writing data to the storage medium; and
>
> a partition defined on the storage medium for dividing the storage medium into a data partition and a secure data partition, the secure data partition for storing secure data and one or more authority records;
>
> wherein only the firmware is permitted to access the secure data and the one or more authority records.

(emphasis added). As previously discussed, the Diamant patent does not teach or disclose "a secure data partition for storing … one or more authority records" as recited in claim 123. The Diamant patent makes no mention of authority records as taught by the claimed invention. Moreover, the Diamant patent does not teach or disclose limiting access to the secure data and the one or more authority records. Further, the Diamant patent does not

teach or disclose permitting "only the firmware", which is part of the storage device, "to access the secure data and the one or more authority records" as recited in the claim.

The Diamant patent teaches controlling access to the secure storage area using an external controller 12 (managing controller 98, and the like) within the server 4 (for example, in FIGS. 1 and 2). Since the external controller operates within the operating system environment of the server 4, the Diamant patent teaches away from the claimed invention, where "only the firmware" of the storage device "is permitted to access the secure data and the one or more authority records" as recited in claim 123. Thus, the Diamant patent does not teach or disclose all the elements of independent claim 123. Therefore, independent claim 123 is novel in view of the cited art. Claims 124-131 and 137 depend from allowable independent claim 123. Therefore, claims 124-131 and 137 are novel in view of the Diamant patent.

B. Claim 129 is Non-Obvious over the Diamant Patent in View of the Aucsmith Patent.

Claim 129 was rejected under 35 U.S.C. 103(a) as being unpatentable over the Diamant patent in view of the Aucsmith patent. The Aucsmith patent is cited for teaching the use of encryption, key pairs, symmetric keys, nonces, and the like.

Both the Diamant patent and the Aucsmith patent teach a controller that is external to the storage device. *See* the Aucsmith patent, Access Controller unit 106 in FIG. 1, for example. *See* also the memory 520 separate from memory 530 in FIG. 5. Both the Aucsmith patent and the Diamant patent teach a controller external to the storage device for controlling access to the storage device via a bus or interface. The Aucsmith patent discloses intimate involvement between the operating system of the computer and the controller as follows:

> Access controller unit 106 receives a process run by processor 104 from mass storage device 103 or another I/O device coupled to bus 100. The process comprises an encrypted executable image and a signature component.

> Before the computer system executes a program, the access controller unit 106 verifies that the signature of the program is legally constructed from a known composite key…

See the Aucsmith patent, col. 4, lines 47-61 (emphasis added). Thus, the access controller unit 106 requires intimate involvement of the operating system of the computer system, which is the type of security problem at least some of the embodiments of the present invention are intended to solve. The access controller unit 106 of the Aucsmith patent is not designed to limit operating system access to a security partition, but rather to verify process requests and executable requests before the operating system executes them.

The combination of the Diamant patent with the Aucsmith patent does not teach, suggest, or disclose the claimed invention. The combination would result in a device external to the storage device for controlling access to the secured data area, since both Aucsmith and Diamant disclose devices external to the storage device for controlling access. In both instances, the external device operates within an operating system environment that is within an operating system of, for example, a server 4 (in Diamant). The asserted combination actually teaches away from the claimed invention, because access decisions are rendered by the external device from within the operating system environment. Thus, the combination of the Diamant patent with the Aucsmith patent does not teach, suggest or disclose restricting access to the secured data area or security partition such that only the firmware can access the secured data area. Consequently, the combination of the Diamant patent with the Aucsmith patent does not teach the claimed invention.

Additionally, it is important to note that in the Diamant patent the controller device (28, 38, 48, 300, or 400 "generates a security key" and provides it to the CPU along with

analysis software from the secured area. The Diamant patent reads as follows:

> "The security key is preferably generated according to a momentary data situation in the secured area 32. The security key can also be generated as a one time key which is independent of the secured area 320, such as according to an internal random generator and the like. The main reason for this is to minimize and preferably eliminate all possible access to this security key from elements which are not authorized and which may attempt to try to provide this key to the processor 302."

See Col. 12, line 33 through Col. 13, line 22 (emphasis added). While it is unclear what is meant by momentary data situation, it is clear that the key is intended for temporary storage or expiration only. By contrast, the Aucsmith patent discloses "a set of keys that are associated with access rights within the computer system" which are stored in access controller unit 106 (*See* Col. 4, lines 37-40). The Aucsmith patent teaches permanent storage of the set of keys in the access controller unit 106. The permanent key storage of the Aucsmith patent cannot be combined with the "momentary data situation" of the Diamant patent without resolving this "permanent versus temporary storage" contradiction. The Diamant patent avoids storing the keys so as to minimize or eliminate unauthorized access to the keys. Consequently, the Diamant patent teaches away from the permanent key storage of the Aucsmith patent. It is not obvious to make the suggested combination, since the Aucsmith patent teaches away from the momentary data situation of the Diamant patent.

Moreover, the Aucsmith patent does not teach public-private key pairs as recited in claim 129. The Aucsmith patent reads as follows:

> The keys can either be private symmetric-keys or public asymmetric-keys. The difference is the extent of protection required by the operating system's copy of the key.

See Col. 5, lines 14-16. Thus, it is not clear that the Aucsmith patent even contemplates a public-private key pair, since the keys are either private and symmetric or public and asymmetric.

Additionally, there is no suggestion or teaching in either reference to make the suggested combination. The alleged "obviousness" of the combination of the key pairs of the Aucsmith patent with controller of the Diamant patent constitutes nothing more than a hindsight reconstruction based on the present application, which discloses key pairs and encryption in combination with security partitions on a storage device, to which access by the operating system is limited. There is no suggestion in either reference to make the asserted combination or to restrict access to a security partition by the operating system as recited by the claimed invention. None of the cited references alone, or in combination, teach, suggest, or disclose "at least one authority record and at least one data set associated with said authority record" and "limiting access to the security partition of said storage device by said operating system of said computer system" of the claimed invention.

Since the keys in the two references teach away from one another (permanent storage versus "momentary data situation"), since the Aucsmith reference does not teach, suggest, or disclose public-private key pairs, since the asserted combination teaches away from the claimed invention, and since there is no teaching in either reference to make the suggested combination, the combination of the Diamant patent and the Aucsmith patent is inappropriate, and should be withdrawn.

Based on the arguments stated above, the Diamant patent in view of the Aucsmith patent does not teach, suggest or disclose the claimed invention as recited in claim 129. Claim 129 is allowable over the cited combination.

Group IV.

Claims 1-15, 20-24, 28, 29, 32-42, 46-49, 53-70, 75-78, 82, 83, 86-103, 108-112, 116, 117, 120-122, 138-139 were rejected under 35 U.S.C. 102(e) as being anticipated by the Diamant patent. Claim 140 was not specifically rejected, but is assumed to be included with the rejection of claims 138-139.

Claims 16-19, 25-27, 30, 31, 43-45, 50-52, 71-74, 79-81, 84, 85, 104-107, 113-115, 118 and 119 were rejected under 35 U.S.C. 103(a) as being unpatentable over the Diamant patent in view of the Aucsmith patent.

Independent claim 1 is directed to a method; independent claim 35 is directed to a system; independent claim 56 is directed to a computer-readable medium containing instruction; and independent claim 89 is written with means-plus-function language. The independent claims 1, 35, 56 and 89 and their associated dependent claims are grouped because the claims are not anticipated by the cited art based on similar claim terms.

A. Group IV Claims are Novel in View of Diamant.

Each of these independent claims recites a computer system having an operating system in operative connection with at least one storage device. An example of this embodiment of the present invention is shown, for example, in FIG. 1, where the computer system 6 has an operating system 10 in operative connection with storage device 12. Each of these independent claims also recites the storage device being partitioned to form a security partition having at least one authority record and at least one data set associated with the authority record. An example of this feature is shown in FIG. 3, where the storage device 30 has an OS file system 42 separated from the authority records 34-38 and security partition (SP) data 32 within the security partition. An authority record is shown in detail, for example, in FIG. 4 and identified generally by reference numeral 52. Additionally, each of these independent claims recites limiting access to the security partition by the operating system

of the computer system. An example of this feature is described in the present application as follows:

> an operating system ("OS") file system 42 is not permitted to access the security partition data 32 contained in the storage device 30.

See Application, p. 10, lines 16-18. Additionally, some applications of these embodiments solve the security problem detailed in the background of the present invention as follows:

> Perhaps the greatest fundamental problem with conventional computer security systems is that their operation is common to the environment of the operating system environment. Furthermore, the operating system environment for many computer systems is also common to the Internet environment, for example, or another network communications medium. Because of this common environment, many means of attack on a computer system are available merely by moving computer code from the Internet to the computer operating system.
>
> ...
>
> Other conventional security systems may include a security device connected to an SCSI bus that protects storage devices on the bus. This type of security system recognizes that the storage device is more secure while not operating in an environment common to the operating system. However, the SCSI bus of this system exposes all devices on the bus, including the storage devices, to access and therefore requires intimate operating systems involvement.

See Application, p. 2, lines 1-20. An embodiment of the present invention limits access by the operating system of the computer system to the secure data within the secure partition. Thus, an embodiment of the present invention provides improved security over an SCSI bus-type security system, which would involve operating systems involvement. Such a conventional external security system operates within the operating system environment and is therefore susceptible to many means of attack, such as by moving malicious computer code from a network to the computer operating system.

The Diamant patent represents just such a conventional security system. In particular, the Diamant patent teaches, for example, in FIGS. 1-4, 6, 7, 9-12 and 14 a controller that is external to the storage device for controlling access to the data stored on the storage device. This external controller (for example, controller 12 in FIG. 1, managing controller 98 in FIG. 2, and so on) is coupled to public network 6 and secured network 8, operates within server 4, and communicates with the storage device 14 via I/O interface 96. *See* the Diamant patent, Col. 7, line 60 through Col. 8, line 25). Moreover, the operating system of server 4 is common to the Internet. The Diamant patent reads as follows:

> The public network 6 is also connected to an external network which in the present example is the Internet 80.

See the Diamant patent, col. 5, lines 35-37. Thus, the Diamant patent teaches a type of controller, which the present disclosure identifies as a security problem (*See* present disclosure, p. 2, lines 3-5).

The Office Action states that the Diamant patent teaches "the secure partition for storing secure data and one or more authority records" citing to Col. 8 line 26- Col. 9, line 31, Col. 10, lines 18-53, Col. 18 line 5-12 and col. 21, lines 1-12. First, this is a misstatement of the recited claim language which reads "a security partition having at least one authority record and at least one data set associated with said authority record". In one embodiment, the authority record is shown, for example, as authority record 52 in FIG. 4. As previously discussed, the authority record 52 includes access rights 56, security partition name 58, passcode 60, public key out 62, public key in 64, symmentric key 66, write permission 68-72, read permissions 74-78, time field 80, encryption settings 82, start, size and number information 84, and secure data 54 associated with the authority record.

Appellant notes that the reference at Col. 8-Col. 9, Col. 10, and Col. 21 relate to the Diamant external controller. The Diamant patent at col. 8 line 26 through Col. 9 line 31 describes a controller adapted to deny access requests for access to secured data received from a public network (*See* Col. 9, lines 3-8 and lines 15-20). The Diamant patent at col. 10 lines 18-53 describes an external device 300 that has a processor 302 for controlling switch 304 "so as to allow or deny access to the secured area 320". *See* Col. 10, lines 47-48. The Diamant patent at col. 18 line 5-12 describes a secured area 1130 containing "data and software which are confidential" and a separate password area 1133 containing "passwords which may be utilized during various procedures by the managing controller 1122, such as switching between modes and the like." The Diamant patent at col. 21, lines 1-12 describes how the "managing controller 1122 connects between the secured area 1130 and the computer 1102, thus enabling the computer to load an operating system from the secured area 1130." The cited portion at Col. 18 lines 5-12 relate to passcodes, which are stored in a passcode area 1133 area of the storage device 1124 in FIG. 14. The passcode information is stored separately from the secured area 1130 and apparently without association to the secured area 1130. The Diamant patent does not teach or disclose storage of passcodes or of authority records within the secure data area as recited in independent claim 141.

Finally, with respect to independent claims 1, 35, 56 and 89, each of the independent claims recites limiting access to the security partition by the operating system of the computer system. The managing controller 98 or controller 12 of the Diamant patent is external to the storage device, operates within the server 4, and is therefore under the control of or intimately involved with the operating system of the computer system. At Col 21, lines 1-12, the managing controller 1122 is responsible

for loading the operating system. Thus, the Diamant patent does not teach or disclose limiting access to the security partition by the operating system. In fact, the Diamant patent describes the controller facilitating switching between operating systems by controlling the loading of the operating system into the computer system, which suggests intimate interaction between the controller and the operating system. *See* Col. 18, lines 46-52.

Thus, the Diamant patent does not teach or disclose a security partition having an authority record and a data set associated with the authority record or limiting access to the security partition by the operating system as recited by the present invention. Therefore, claims 1, 35, 56, and 89 and their associated dependent claims are believed to be novel over the Diamant patent.

B. Group IV Claims Are Non-Obvious in View of the Diamant Patent and the Aucsmith Patent.

Claims 16-19, 25-27, 30, 31, 43-45, 50-52, 71-74, 79-81, 84, 85, 104-107, 113-115, 118 and 119 were rejected under 35 U.S.C. 103(a) as being unpatentable over the Diamant patent in view of the Aucsmith patent. As previously discussed, the Aucsmith patent is cited for public and private keys. However, as previously discussed, since the keys in the two references teach away from one another (permanent storage versus "momentary data situation"), since the Aucsmith reference does not teach, suggest, or disclose public-private key pairs, since the asserted combination teaches away from the claimed invention, and since there is no teaching in either reference to make the suggested combination, the combination of the Diamant patent and the Aucsmith patent is inappropriate, and should be withdrawn.

Moreover, the asserted combination teaches away from the present invention, as recited in the claims, because access decisions are rendered by an external device from within the operating system environment. Therefore, access to the secured area or security partition by the operating system is not

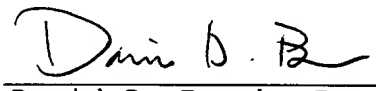
limited. By contrast, independent claims 1, 35, 56 and 89, from which claims 16-19, 25-27, 30, 31, 43-45, 50-52, 71-74, 79-81, 84, 85, 104-107, 113-115, 118 and 119 depend, recites that access by the operating system is limited. Thus, the combination of the Diamant and the Aucsmith patents do not teach, suggest or disclose all the elements of claims 16-19, 25-27, 30, 31, 43-45, 50-52, 71-74, 79-81, 84, 85, 104-107, 113-115, 118 and 119, which are therefore allowable over the cited combination. The rejection of claims 16-19, 25-27, 30, 31, 43-45, 50-52, 71-74, 79-81, 84, 85, 104-107, 113-115, 118 and 119 over a combination of the Diamant patent with the Aucsmith patent under 35 U.S.C. 103(a) is overcome.

CONCLUSION

Appellants respectfully submit that claims 1-145 are allowable over the prior art. None of the cited references alone, or in combination, teach, suggest, or disclose all the elements of the independent claims of the present application. Appellants therefore request reversal of the rejection of claims 1-145. Favorable action is solicited.

Respectfully submitted,

WESTMAN, CHAMPLIN & KELLY, P.A.

By: 

David D. Brush, Reg. No. 34,557
Suite 1600 - International Centre
900 Second Avenue South
Minneapolis, Minnesota 55402-3319
Phone:(612) 334-3222 Fax:(612) 334-3312

DDB/RMR:rkp

Appendix A

CLAIMS AS PRESENTLY PENDING:

1. (Previously Amended) A method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device, and said method comprising:

partitioning at least a portion of said storage device to form a security partition having at least one authority record and at least one data set associated with said authority record; and

limiting access to the security partition of said storage device by said operating system of said computer system.

2. (Original) The method of Claim 1, wherein said computer system includes a networked computer system.

3. (Original) The method of Claim 1, wherein at least a portion of said storage device firmware comprises writeable firmware.

4. (Original) The method of Claim 1, wherein at least a portion of said storage device firmware comprises non-writeable firmware.

5. (Original) The method of Claim 1, further comprising transporting data to said storage device only in connection with execution of said firmware of said storage device.

6. (Original) The method of Claim 1, wherein said storage device is configured in accordance with a protocol selected from the group consisting of ATA protocol and SCSI protocol.

7. (Original) The method of Claim 1, wherein said partitioning steps occurs on a low-level formatting portion of said storage device.

8. (Original) The method of Claim 1, further comprising adding data to said storage device in an orientation selected for promoting identification of remaining data storage space on said storage device.

9. (Original) The method of Claim 1, further comprising said security partition having a master authority record.

10. (Original) The method of Claim 9, further comprising said master authority record governing all said authority records in said storage device.

11. (Original) The method of Claim 1, further comprising translating information from a master authority record included in said storage device to a group authority in said operating system.

12. (Original) The method of Claim 1, further comprising writing said security partition using a security partition open call.

13. (Original) The method of Claim 12, further comprising closing said security partition after a predetermined time interval.

14. (Original) The method of Claim 1, further comprising reading said security partition using a security partition open call.

15. (Original) The method of Claim 14, further comprising closing said security partition after a predetermined time interval.

16. (Original) The method of Claim 1, wherein said authority record includes a public-private key pair for authenticating data originating from said security partition.

17. (Original) The method of Claim 16, wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data.

18. (Original) The method of Claim 1, further comprising storing a symmetric key on said storage device.

19. (Original) The method of Claim 1, further comprising using a private key for decoding a passcode transmitted to said authority record of said storage device.

20. (Original) The method of Claim 1, further comprising encrypting at least a portion of said data in said security partition.

21. (Original) The method of Claim 1, further comprising encrypting data on said storage device so that only an external agent can decrypt said encrypted data.

22. (Original) The method of Claim 1, further comprising providing no method for decrypting data stored on said storage device with information available on said storage device.

23. (Original) The method of Claim 1, further comprising hiding at least one field of said authority record.

24. (Original) The method of Claim 1, further comprising storing

a hash of code in a passcode field of said authority record.

25. (Original) The method of Claim 1, further comprising securing a symmetric key by encrypting said symmetric key with a public key of said authority record, and hiding a private key in said authority record, thereby permitting only said hidden private key to decode said symmetric key.

26. (Original) The method of Claim 1, further comprising storing at least one public key in said storage device.

27. (Original) The method of Claim 1, further comprising storing at least one private key in said storage device.

28. (Original) The method of Claim 1, further comprising declaring at least a portion of data in said security partition to be write-once.

29. (Original) The method of Claim 1, further comprising permitting only a predetermined user to access a master authority record of said security partition.

30. (Original) The method of Claim 1, wherein said authority record includes at least one nonce.

31. (Original) The method of Claim 30, further comprising encrypting said nonce with a public key.

32. (Original) The method of Claim 1, wherein said authority record includes at least one time value associated with processing of a portion of data stored on said storage device.

33. (Original) The method of Claim 32, wherein said time value is

selected from the group consisting of a start time and an end time.

34. (Original) The method of Claim 1, further comprising storing call authentication data on said storage device.

35. (Original) A system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device, said system for promoting security comprising:

a security partition formed in said storage device having at least one authority record and at least one data set associated with said authority record;

wherein access to said partition in said storage device by said operating system of said computer system is limited.

36. (Original) The system of Claim 35, wherein said computer system includes a networked computer system.

37. (Original) The system of Claim 35, wherein at least a portion of said storage device firmware comprises writeable firmware.

38. (Original) The system of Claim 35, wherein at least a portion of said storage device firmware comprises non-writeable firmware.

39. (Original) The system of Claim 35, wherein said storage device is configured in accordance with a protocol selected from the group consisting of ATA protocol and SCSI protocol.

40. (Original) The system of Claim 35, wherein said security partition is formed on a low-level formatting portion of said storage device.

41. (Original) The system of Claim 35, further comprising said security partition having a master authority record.

42. (Original) The system of Claim 41, further comprising said master authority record being in operative association with a group authority in said operating system.

43. (Original) The system of Claim 35, wherein said authority record includes a public-private key pair for ensuring data can only be sent to said security partition.

44. (Original) The system of Claim 43, wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data.

45. (Original) The system of Claim 35, further comprising a symmetric key stored on said storage device.

46. (Original) The system of Claim 35, further comprising encrypted data stored on said storage device.

47. (Original) The system of Claim 35, further comprising at least one hidden field in said authority record.

48. (Original) The system of Claim 35, further comprising said authority record having a passcode field.

49. (Original) The system of Claim 35, further comprising a hidden key stored in said storage device.

50. (Original) The system of Claim 35, further comprising at

least one public key stored in said storage device.

51. (Original) The system of Claim 35, further comprising at least one private key stored in said storage device.

52. (Original) The system of Claim 35, wherein said authority record includes at least one nonce.

53. (Original) The system of Claim 35, wherein said authority record includes at least one time value associated with processing of a portion of data stored on said storage device.

54. (Original) The system of Claim 53, wherein said time value is selected from the group consisting of a start time and an end time.

55. (Original) The system of Claim 35, further comprising call authentication data stored on said storage device.

56. (Original) A computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device, said medium comprising:

instructions for partitioning at least a portion of said storage device to form a security partition having at least one authority record and at least one data set associated with said authority record;

instruction for limiting access to at least a portion of said storage device by said operating system of said computer system.

57. (Original) The medium of Claim 56, wherein said computer system includes a networked computer system.

58. (Original) The medium of Claim 56, wherein at least a portion of said storage device firmware comprises writeable firmware.

59. (Original) The medium of Claim 56, wherein at least a portion of said storage device firmware comprises non-writeable firmware.

60. (Original) The medium of Claim 56, further comprising instructions for transporting data to said storage device only in connection with execution of said firmware of said storage device.

61. (Original) The medium of Claim 56, wherein said storage device is configured in accordance with a protocol selected from the group consisting of ATA protocol and SCSI protocol.

62. (Original) The medium of Claim 56, wherein said instruction for partitioning include instruction for partitioning in a low-level formatting portion of said storage device.

63. (Original) The medium of Claim 56, further comprising instructions for adding data to said storage device in an orientation selected for promoting identification of remaining data storage space on said storage device.

64. (Original) The medium of Claim 56, further comprising said security partition having a master authority record.

65. (Original) The medium of Claim 64, further comprising said master authority record including instructions for governing all said authority records in said storage device.

66. (Original) The medium of Claim 56, further comprising instructions for translating information from a master authority record included in said storage device to a group authority in said operating system.

67. (Original) The medium of Claim 56, further comprising instructions for writing said security partition using a security partition open call.

68. (Original) The medium of Claim 67, further comprising instructions for closing said security partition after a predetermined time interval.

69. (Original) The medium of Claim 56, further comprising instructions for reading said security partition using a security partition open call.

70. (Original) The medium of Claim 69, further comprising instructions for closing said security partition after a predetermined time interval.

71. (Original) The medium of Claim 56, wherein said authority record includes a public-private key pair for authenticating data originating from said security partition.

72. (Original) The medium of Claim 71, wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data.

73. (Original) The medium of Claim 56, further comprising instructions for storing a symmetric key on said storage device.

74. (Original) The medium of Claim 56, further comprising instructions for using a private key for decoding a passcode transmitted to said authority record of said storage device.

75. (Original) The medium of Claim 56, further comprising instructions for encrypting at least a portion of said data in said security partition.

76. (Original) The medium of Claim 56, further comprising instructions for encrypting data on said storage device so that only an external agent can decrypt said encrypted data.

77. (Original) The medium of Claim 56, further comprising instructions for hiding at least one field of said authority record.

78. (Original) The medium of Claim 56, further comprising instructions for storing a hash of code in a passcode field of said authority record.

79. (Original) The medium of Claim 56, further comprising instructions for securing a symmetric key by encrypting said symmetric key with a public key of said authority record, and instructions for hiding a private key in said authority record, thereby permitting only said hidden private key to decode said symmetric key.

80. (Original) The medium of Claim 56, further comprising instructions for storing at least one public key in said storage device.

81. (Original) The medium of Claim 56, further comprising

instructions for storing at least one private key in said storage device.

82. (Original) The medium of Claim 56, further comprising instructions for declaring at least a portion of data in said security partition to be write-once.

83. (Original) The medium of Claim 56, further comprising instructions for permitting only a predetermined user to access a master authority record of said security partition.

84. (Original) The medium of Claim 56, wherein said authority record includes at least one nonce.

85. (Original) The medium of Claim 84, further comprising instructions for encrypting said nonce with a public key.

86. (Original) The medium of Claim 56, wherein said authority record includes at least one time value associated with processing of a portion of data stored on said storage device.

87. (Original) The medium of Claim 86, wherein said time value is selected from the group consisting of a start time and an end time.

88. (Original) The medium of Claim 56, further comprising of instructions for storing call authentication data on said storage device.

89. (Previously Amended) A system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data

stored on said storage device, said system for promoting security comprising:

means for partitioning at least a portion of said storage device to form a security partition having at least one authority record and at least one data set associated with said authority record; and

means for limiting access to the security partition of said storage device by said operating system of said computer system.

90. (Original) The system of Claim 89, wherein said computer system includes a networked computer system.

91. (Original) The system of Claim 89, wherein at least a portion of said storage device firmware comprises writeable firmware.

92. (Original) The system of Claim 89, wherein at least a portion of said storage device firmware comprises non-writeable firmware.

93. (Original) The system of Claim 89, further comprising means for transporting data to said storage device only in connection with execution of said firmware of said storage device.

94. (Original) The system of Claim 89, wherein said storage device is configured in accordance with protocol selected from the group consisting of ATA protocol and SCSI protocol.

95. (Original) The system of Claim 89, wherein said means for partitioning partitions a low-level formatting portion of said storage device.

96. (Original) The system of Claim 89, further comprising means

for adding data to said storage device in an orientation selected for promoting identification of remaining data storage space on said storage device.

97. (Original) The system of Claim 89, further comprising said security partition having a master authority record.

98. (Original) The system of Claim 97, further comprising means for said master authority record to govern all said authority records in said storage device.

99. (Original) The system of Claim 89, further comprising means for translating information from a master authority record included in said storage device to a group authority in said operating system.

100. (Original) The system of Claim 89, further comprising means for writing said security partition using a security partition open call.

101. (Original) The system of Claim 100, further comprising means for closing said security partition after a predetermined time interval.

102. (Original) The system of Claim 89, further comprising means for reading said security partition using a security partition open call.

103. (Original) The system of Claim 102, further comprising means for closing said security partition after a predetermined time interval.

104. (Original) The system of Claim 89, wherein said

authority record includes a public-private key pair for authenticating data originating from said security partition.

105. (Original) The system of Claim 104, wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data.

106. (Original) The system of Claim 89, further comprising means for storing a symmetric key on said storage device.

107. (Original) The system of Claim 89, further comprising means for using a private key for decoding a passcode transmitted to said authority record of said storage device.

108. (Original) The system of Claim 89, further comprising means for encrypting at least a portion of said data in said security partition.

109. (Original) The system of Claim 89, further comprising means for encrypting data on said storage device to that only an external agent can decrypt said encrypted data.

110. (Original) The system of Claim 89, further comprising means for providing no system for decrypting data stored on said storage device with information available on said storage device.

111. (Original) The system of Claim 89, further comprising means for hiding at least one field of said authority record.

112. (Original) The system of Claim 89, further comprising means for storing a hash of code in a passcode field of said authority record.

113. (Original) The system of Claim 89, further comprising means for securing a symmetric key by encrypting said symmetric key with a public key of said authority record, and means for hiding a private key in said authority record, thereby permitting only said hidden private key to decode said symmetric key.

114. (Original) The system of Claim 89, further comprising means for storing at least one public key in said storage device.

115. (Original) The system of Claim 89, further comprising means for storing at least one private key in said storage device.

116. (Original) The system of Claim 89, further comprising means for declaring at least a portion of data in said security partition to be write-once.

117. (Original) The system of Claim 89, further comprising means for permitting only a predetermined user to access a master authority record of said security partition.

118. (Original) The system of Claim 89, wherein said authority record includes at least one nonce.

119. (Original) The system of Claim 118, further comprising means for encrypting said nonce with a public key.

120. (Original) The system of Claim 89, wherein said authority record includes at least one time value associated with processing of a portion of data stored on said storage device.

121. (Original) The system of Claim 120, wherein said time

value is selected from the group consisting of a start time and an end time.

122. (Original) The system of Claim 89, further comprising means for storing call authentication data on said storage device.

123. (Previously Added) A storage device for promoting security in a computer system, the storage device comprising:

a storage medium for storing data;

firmware for reading data from and writing data to the storage medium; and

a partition defined on the storage medium for dividing the storage medium into a data partition and a secure data partition, the secure data partition for storing secure data and one or more authority records;

wherein only the firmware is permitted to access the secure data and the one or more authority records.

124. (Previously Added) The storage device of claim 123 wherein the one or more authority records includes one master authority record.

125. (Previously Added) The storage device of claim 123 wherein the storage device is in communication with a computer system having an operating system.

126. (Previously Added) The storage device of claim 125, wherein secure data stored in the secure data partition is invisible to the operating system.

127. (Previously Added) The storage device of claim 123, wherein

the one or more authority records define access permissions relating to the secure data partition and the secure data.

128. (Previously Added) The storage device of claim 127, wherein the secure data partition contains a master authority record, wherein the one or more authority records can be created and deleted as required by a user having access permissions according to the master authority record.

129. (Previously Added) The storage device of claim 123 wherein each of the one or more authority records contains one public-private key pair for authenticating data that originates from the security partition.

130. (Previously Added) The storage device of claim 123, wherein the storage device further comprises:

cryptographic operations embedded in the firmware of the storage device.

131. (Previously Amended) The storage device of claim 130, wherein cryptographic code is authenticated with a root assurance in the firmware of the device, wherein the firmware is non-writable.

132. (Previously Added) A method for promoting security in a computer system having an operating system in operative connection with a storage device, wherein said storage device includes a processor and firmware for processing data stored on the storage device, the method comprising:

partitioning a storage medium of the storage device into a data partition and a secure data partition, the data partition being accessible to a user and the secure data partition being invisible to the

user, the secure data partition for storing secure data and one or more authority records; and

restricting access to the secure data partition such that only the firmware may access the secure data and the one or more authority records.

133. (Previously Added) The method of claim 132, further comprising:

prohibiting access to the secure data partition by the operating system of the computer system.

134. (Previously Added) The method of claim 133, wherein a portion of the firmware is non-writable.

135. (Previously Added) The method of claim 132, further comprising:

writing data to the secure data partition by executing of a portion of the firmware of the storage device; and

associating the data with a particular record of the one or more authority records.

136. (Previously Added) The method of claim 132 wherein the secure data is encrypted and wherein cryptographic code is embedded in the firmware, the method further comprising: authenticating the cryptographic code with a root assurance in the storage device.

137. (Previously Amended) The storage device of claim 123, wherein the secure data is accessed by the firmware using a security partition open call internal to the storage device and hidden from a user.

138. (Previously added) The system of claim 89 wherein the means for partitioning comprises a computer readable medium containing instructions for partitioning the storage device.

139. (Previously added) The system of claim 89 wherein the means for limiting access to the security partition comprises the processor within the storage device, the processor adapted to limit access to the security partition according to the at least one authority record.

140. (Previously added) The system of claim 89 wherein the means for limiting access to the security partition comprises the firmware within the storage device, the firmware adapted to limit access to the security partition according to the at least one authority record.

141. (Previously added) A storage device comprising:

a storage medium having a security partition containing one or more authority records and at least one data set associated with each of the one or more authority records; and

a mechanism within the storage device adapted to limit access to the security partition based on the one or more authority records.

142. (Previously added) The storage device of claim 141 wherein the mechanism comprises:

a processor disposed within the storage device adapted to limit access to the security partition by an operating system of a computer system.

143. (Previously added) The storage device of claim 141 wherein the mechanism comprises:

firmware disposed within the storage device adapted to limit access to the security partition by an operating system of a computer system.

144. (Previously added) The storage device of claim 141 wherein the one or more authority records comprises a master authority record including instructions for governing the one or more authority records in said storage device.

145. (Previously added) The storage device of claim 141 wherein each of the one or more authority records comprises a plurality of fields, wherein a first field of the plurality of fields contains access rights governing access to the at least one data set.